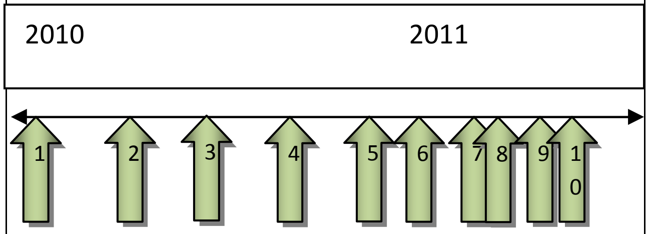
Data Loss Prevention Project Summary

for ITRMC Review

Date Submitted:		Agency Director:	Mike Gwartney
Agency:	Dept of Administration	Project Number:	
Project Name:	Enterprise Data Loss Protection		
Project Manager:	Terry Pobst-Martin		
Total Project Budget:		Project Start Date:	Spring 2010
Is project currently funded? Y or N	N	Estimated End Date:	March 2012
Executive Sponsor:	Greg Zickau		

Description	Deliverable
1. Project Summary. The State of Idaho is transmitting sensitive data via unsecure means to locations which are not controlled. This problem is not unique to Idaho; many organizations are facing this issue. One successful means to reduce or stop the loss of sensitive information is to employ a Data Loss Protection (DLP, also known as Data Leak Prevention) solution which can see that loss and help us mitigate it. It has become more difficult than ever for any organization to prevent the loss of sensitive data. Most security approaches we've practiced in the past concentrated on just securing the network, not necessarily the data. Newer security tools are focusing on data and applications, and this project is focused on protecting the loss of data. With a DLP, organizations gain visibility into policy violations to proactively secure data with automatic quarantine, relocation, and support for policy-based encryption. A DLP can enable active blocking at both the network and endpoint to prevent confidential data from leaving the organization inappropriately. It can help significantly reduce risk by automatically enforcing compliance with data security policies as well as provide detailed information which enables organizations to change employee behavior.	**A. Type of Project:** Security **B. Detailed Description:** DLP solutions automatically monitor data as it leaves the state network and provides a variety of selective responses when they identify unencrypted sensitive data leaving the network. This type of solution significantly reduces the risk of a data breach from either an outsider who is accessing that data illegally from the Internet, or an insider who is leaking data, innocently or maliciously, and making it vulnerable to theft. Reducing this risk will help prevent the state from losing citizen confidence which often follows a major data breach as well as help reduce the possibility the state will pay the enormous costs associated with the required response to a data breach. **C. Project Charter Statement:** At the successful completion of this project, the state will have assessed, chosen, procured and employed a Data Loss Prevention technical solution which will monitor data as it leaves the state network and will automatically enforce compliance (or automatically notify decision makers of the options to enforce compliance) with specific policies, standards and regulations. The solution will provide clear metrics on the number of data leaks over time. The goal is to reduce the risk of a breach of state-owned data by cutting data loss incidents by 80% within one year. The DLP Program will then follow the project and will enable decreasing data losses each year.

Description	Deliverable
2. Business Case. The state has a clear responsibility to protect the private and personal data of our citizens and employees, as well as other sensitive information such as the proprietary data of our business partners. Right now, we know intentional or unintentional release of sensitive information is occurring from the state network to the Internet. Three companies that manufacture systems called Data Loss Prevention solutions offered to run demonstrations/evaluations at the primary internet connection for the state this summer. Through those product evaluations we know that personal, privacy and financial data is flowing, unencrypted, to the Internet. These initial results show that we have a problem that can only be identified by a solution such as we've had demonstrated. See the **Chart A & B** after this table to see the results from one device reporting losses during August. Among the many state agencies, personal data of almost every Idaho citizen is held in computer databases for various applications. If we lost only 1% of that data in a breach where criminals stole or somehow obtained it, the cost to the state would be significant.	**A. Cost/benefit analysis:** If only 1 % of Idaho citizens were affected by a data breach, the cost, at $230 per record notification costs, would reach $34.5 Mil. The Data Loss Protection will cost, the first year, $530K. That's a savings, initially of almost $34 Mil. See **Chart C** at the end of this table. **B. A description of the risk or mandate:** The risk is that State employee practices or habits are not sufficiently controlled enough to ensure we do not lose citizen or other constituent sensitive data to those who would use that information maliciously. We are required, by statute, to protect sensitive information, to include the following: • SSNs of state employees & all Idaho citizens • Other privacy information • Driver's License Numbers • HIPAA information • Payment Card Industry Data • Financial information • Sensitive government information Identity theft is growing rapidly, and the cost to individuals, businesses, the economy, and to governments is substantial.
3. Budget. The requested budget to implement a DLP solution designed to monitor and mitigate loss of sensitive data over the Internet is $530K	A. Overall budget, subtotaled for each cost category for each fiscal year of the project: a. Hardware: (with software) $400K (One time) $50K (Ongoing) b. Software: See above c. Contracted Services: $80K d. FTP's: N/A e. Training: N/A B. Request is for General Funds, other sources will be considered over time. C. Constraints are considerable in this economic environment. General Funds are not likely to be available. D. One contracted security analyst will be required to manage the system and the agency responses.

Description	Deliverable
4. Schedule, Time Constraints & Dependencies. The first milestone is for OCIO to present this, among other budget requests, to JFAC. If this is included in FY2011 approved budget items, them the true timeline will follow as shown.  2010 2011 1 2 3 4 5 6 7 8 9 10	A. Project Schedule. If funded for FY11, this project should be complete by the end of Q3 FY11, Mar 2011. B. Indicate project milestones: **2010** 1. Spring, Legislature passes funding 2. Apr - Jun, thorough product assessment begins, coordination with agencies 3. Jul, Product assessment finishes & hire DLP Security Analyst 4. Sep, RFP developed 5. Nov, Contract awarded 6. Dec, Product received and initial testing begins; plus, Awareness and Training Campaign start **2011** 7. Jan 15, Initial implementation 8. Jan 30, Initial assessment 9. Feb 20, Full Implementation 10. Mar 1, Monitor and coordinate with agencies **2012** 11. March, 80% reduction in identified losses from initial implementation C. Critical time constraints and dependencies: - Obtaining funding is critical so if the Legislature does not fund this and we have to try to leverage other agencies who want this, the schedule will be slipped considerably. - RFP development could take longer than scheduled or contract award may cause delays if contested.
5. Project Risks. There are few technical risks with the project as planned. The evaluation of the three DLP products showed there are some risks with uptime of a couple of the solutions as tested. We expect full technical support to solve those issues. Other risks involve time required to respond to DLP reports as well as state agencies ability to respond to the results of the DLP reports. Mitigations are planned for each identified risk.	A. Listing of known risks and the mitigation strategy for each. Technical risks: - Risk: System failures as seen during evaluation Mitigation: Ensure vendor provides full technical support for system - Risk: Time to evaluate, disseminate, and follow-up on reports takes considerable time which OCIO may not currently have Mitigation: OCIO will contract out the majority of this additional work while maintaining close oversight.

	- Risk: Agencies may not have the manpower or time to respond to the reports of data leaks originating in their agencies. Mitigation: OCIO will ensure we choose a DLP option that includes highly automated and accurate response options which will significantly reduce the stress on agencies to respond to the data loss instances. - Risk: Agencies may not have the will to modify business practices that lead to some of the data leaks. Mitigation: This project will include an awareness and training campaign developed to ensure agencies understand the benefits of the DLP and how minor modifications to business practices, in response to the reports, will benefit them overall B. Completed Risk Assessment G215 (attached).
6. Possible Solutions/Alternatives. Alternatives will cost the state more in the long run, will take longer to succeed, will not be as accurate as the automated method and will be difficult to enforce.	A. Listing of alternatives considered - Study business practices of individual agencies to determine where improvements are needed to ensure agencies stop loss of business data. Notify each agency of the identified improvements. Help the agencies implement the improvements. This alternative would require additional people over several years to be devoted to this issue and, once complete, would require continued time and resources to audit agency results. This would be much more costly than the planned project and may not mitigate individual mistakes or faulty processes. - Request each agency to completely review its own business practices in a similar manner to the above alternative. This would spread the work to all agencies and would be applied inconsistently so quality control of the process would be impossible. This would also be very costly and may not address all possible data leaks, may not mitigate individual mistakes and is not likely to succeed in some agencies that do not have the resources or desire to affect needed changes. - Individual agencies could install their own DLP solutions and determine their own actions to identify and resolve faulty business practices

	which lead to the loss of sensitive data. This option would be inconsistently applied since each agency would determine their specific goals and employ the solution differently. The manpower required to employ this throughout the state would be much greater than a centralized solution. The cost would be significantly greater if each agency had to purchase its own solution. - Conduct a large-scale awareness campaign of the problems the state agencies have in losing sensitive data. With increased awareness overtime, agencies night independently develop more secure business practices and individuals would develop better work habits and processes for handling sensitive information. This alternative is unrealistic, would yield inconsistent results and may not decrease the state's risk of a data breach for many years, if ever. B. Safeguarding the information on the state network is clearly stated as one of the five goals of the ITRMC approved State of Idaho Information Technology Strategic Plan: Our citizens and businesses have a high expectation that the State will appropriately secure its digital government services and assure the availability, integrity, and confidentiality of their information. We will meet these expectations through secure technology, sound privacy policies and best practices for the protection of information entrusted to the State while providing greater access to convenient government services.
7. Collaboration/Consolidation. There is a strong opportunity for collaboration and consolidation with this project, if agencies were willing to share resources and employ those resources to the benefit of all agencies.	A. List of possible opportunities for collaboration. The very likely possibility of this not being funded by General funds this year could lead specific agencies to pool their resources to ensure the project moves forward. These agencies, particularly those who are most interested in stopping their data loss, would provide a portion of the overall cost from their own budgets in order to pay for the technical solution as well as to pay for a contracted security analyst to manage the

	ongoing program. This option will enable agencies with the most risk and with some resources to address the issue to obtain a state-wide solution at much less overall cost than the combined cost of agencies funding individual solutions.

Chart A Severity of Data Leaks – Based on Likelihood that Loss will Lead to Identity Theft or Other Damaging Crime

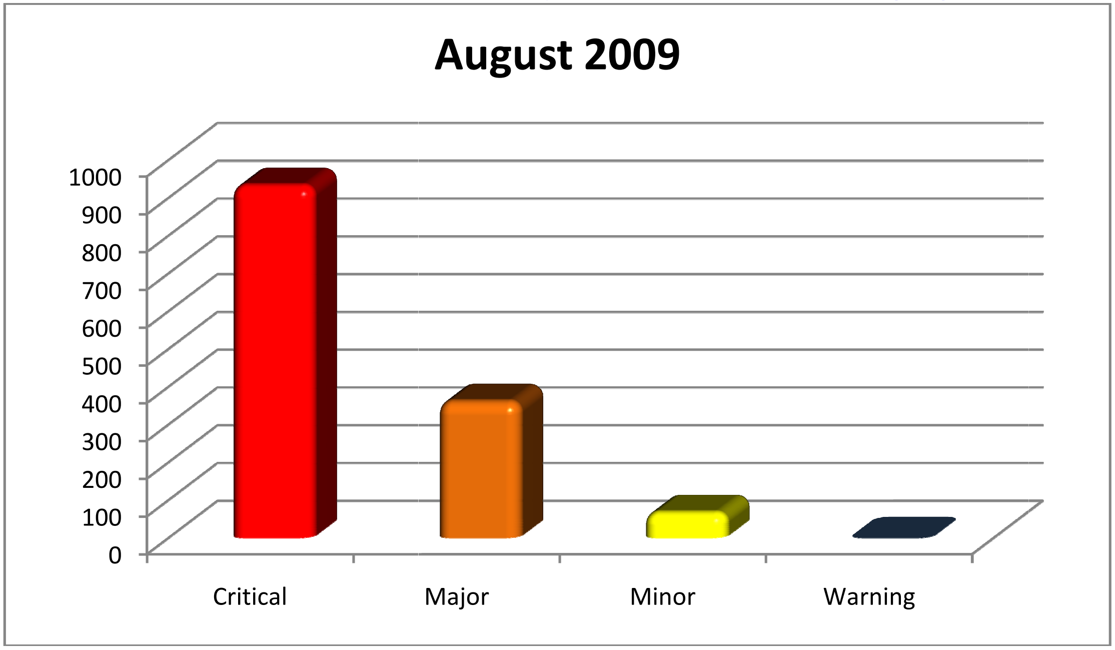


Chart B Type of Information Leaked

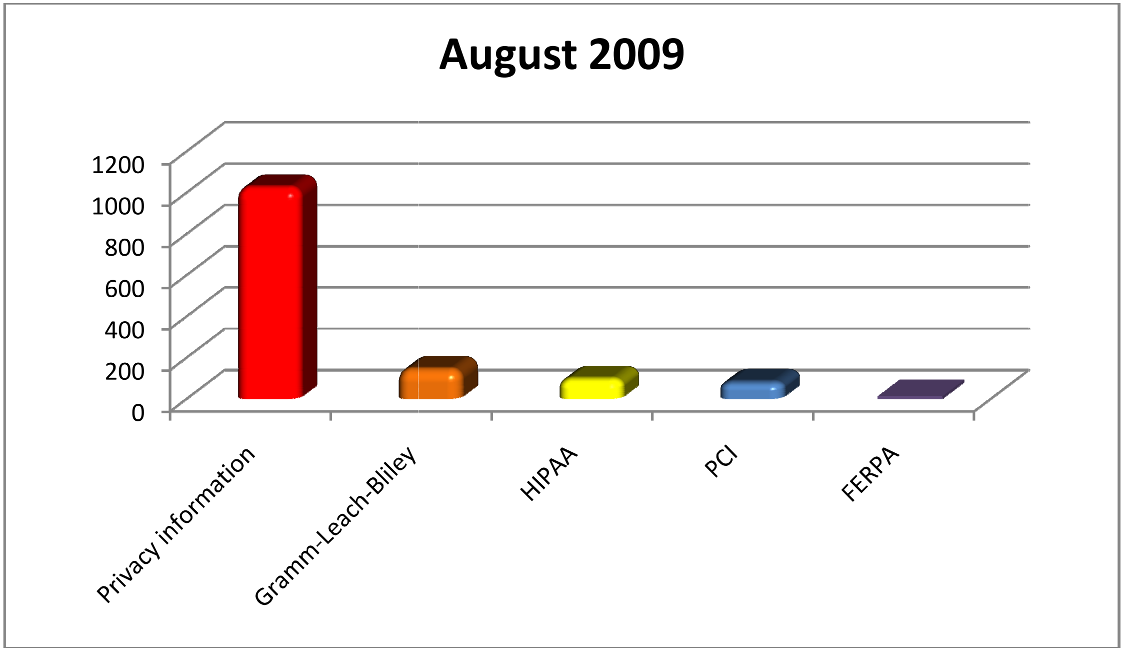


Chart C

Cost Benefit Chart

Approximate 1% of Idaho population	Cost for notification each individual record	Cost of notification	Potential suits for damages	Cost of full DLP solution - network & data at rest	Less robust DLP solution - network
150,000	$230	$34,500,000	uncertain	$680,000	$530,000
			Potential Savings:	$ 33,120,000	$ 33,970,000